システムの記事

Certified Wireless USB プロトコル検証における着眼点

――有線USBにはなかったアソシエーションやパケット構造を考慮

福崎達也

Certified Wireless USBのデバイス層やファンクション層は，ソフトウェアの互換性を維持するため従来の有線のUSBとほとんど同じである．しかし，無線通信特有の干渉などの問題を解決するため，データの暗号化や接続手順，パケット構造などが変更されている．ここでは，こうした従来のUSBとの相違点に焦点を当てながら，Certified Wireless USBのプロトコルの検証方法を解説する．（編集部）

USB（universal serial bus）の無線化には，従来の有線のUSBにはなかった二つの大きな課題がありました．

一つは，干渉してほしくない複数の伝送が同じ空間内で行われる可能性があることです．従来のUSBの場合，近くにある複数のパソコンがUSB対応機器（マウスやハード・ディスク装置）を同時に使ったとしても，何の配慮も必要ありません．しかし，もしこれらが干渉し合うとしたらどうすればよいでしょうか．その回避策として，USB-IF（Implementers Forum）は「アソシエーション」という接続手順を策定しました（詳細は後述）．

二つ目は，パケット・エラー率（PER）がこれまでの有線のUSBに対して格段に悪い（高い）ことです．有線のUSBでは，ホストがデバイスに話しかけ，デバイスはNAK信号（再送要求）かACK信号（正常受信）を返します．しかし，無線化されたUSBではPERが悪いため，有線のUSBのような頻繁にやりとりする仕組みではうまく機能しません．そこで，Certified Wireless USB[注1]（以下，Wireless USBとする）ではMMC（micro-scheduled management commands）と呼ばれる単一の制御パケットにすべてのトークンを集約しています．

ここでは，こうした従来の有線のUSBとの相違点を踏まえて，Wireless USBの論理層の検証について説明します．

1．プロトコル検証のポイント

Wireless USBのプロトコル検証で重要なポイントは，使用するチップ・セットの構成，および暗号化やアソシエーション・モデルなどへの対応です．

● チップ構成に応じたテスト環境を築く

初期のWireless USB対応チップ・セットは，RF IC（物理層）とMAC（media access control）ICから構成されていました．そのためテストする場合も，RF ICとMAC ICを接続するための標準的なピン配置を定義したMPI（MAC-PHY Interface）から信号を取り出し，データの解析を行うのが一般的でした．

しかし，今ではICの開発が進み，RF部とMACを1チップに集積したLSIが製品化されています．また無線ベースの相互接続性，Wireless USBプロトコル・タイミング，MMCやCTA（channel time allocation；デバイスがホストと通信するためのスケジューリングを行う）のタイミングなどについての検証が重要となってきました．そこでプロトコル検証には，次の三つのアプローチが必要となっています．

注1：Certified Wireless USBは，無線方式としてWiMedia Allianceが定める MB-OFDM（multiband-orthogonal frequency division modulation）を用いた無線USB規格．2005年5月にUSB-IFにてその仕様が承認された．

KeyWord　Certified Wireless USB，WiMedia Alliance，MB-OFDM，MMC，CTA，アソシエーション・モデル，PLCP

1）MPIベースのデータ捕捉

RF ICとMAC ICの間に流れるデータを有線で捕捉する方法です（**図1**）．現在でもプロトタイプのデバイスは，MACとRFが分離されていることが少なくありません．RF ICとMAC ICの開発元が別会社というケースも多いので，それらのICの接続性を確認するためにMPIベースのデータ補足は重要です．

2）無線ベースのデータ捕捉 注2

空中伝播（over-the-air）によるデータの捕捉は，実際の利用環境にもっとも近いテスト方式です（**図2**）．無線ベースとMPIベースで同時にデータを捕捉できるプロトコル・アナライザを用いれば，不ぐあいが発生した場合に無線化された際のエラーなのか，物理層へのデータの入力段階におけるエラーなのかを切り分けることができます（**写真1**）．

3）SMA（同軸）ケーブルによるデータ捕捉

この方法では，減衰器を挿入したケーブルとスプリッタ（分波器）を利用します（**図3**）．ノイズの多いテスト環境では，SMAケーブルで直接接続してデータを捕捉します．電波を空中に出さないので，テストのために無線局の免許注3を取得する必要はありません．

● 実際のフレームとアナライザ表示の対応

Wireless USBのパケット構造を**図4**に示します．先頭にPLCP（PHY Layer Convergence Protocol）プリアンブルがあります(5)．PLCPヘッダは53 Mbpsでエンコードされていますが，将来の拡張用に確保しているビットを含んでいます．ペイロードは53Mbps～480Mbpsの伝送速度でエンコードされます．それぞれのフレームはMB-OFDM

注2：電波を出さないため測定対象に影響を与えない“sniffer（盗聴）”と呼ばれる方式を用いる．
注3：無線通信による実機の評価は，総務省が定める電波法にのっとって行う必要がある．

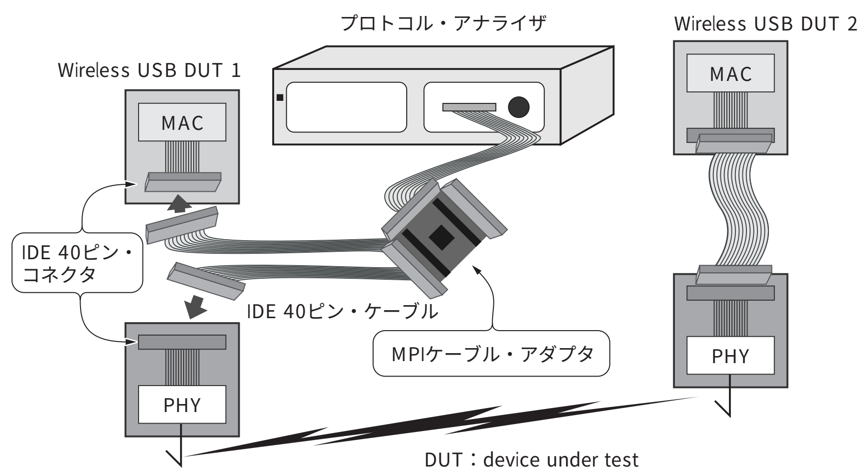


図1
MPIベースのデータ捕捉
FR ICとMAC ICの間のデータを捕捉する方式．

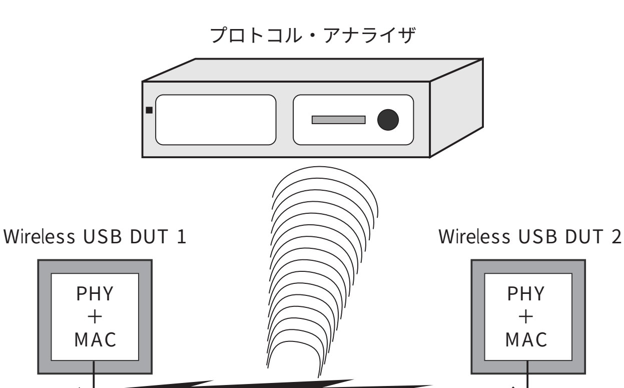


図2　無線ベースのデータ捕捉
DUT（テスト対象デバイス）どうしで行っている無線通信のデータを，プロトコル・アナライザが捕捉する．実際の利用環境にもっとも近い方式．

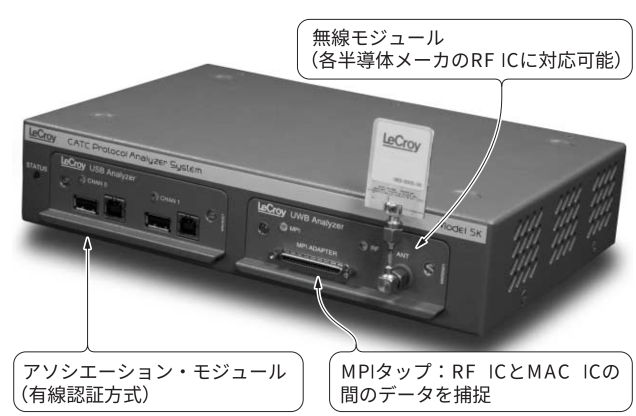


写真1　Wireless USB対応のプロトコル・アナライザ
写真は，米国LeCroy社のCertified Wireless USB対応プロトコル・アナライザ「UWB Tracer」．無線部分をプラグイン形式のモジュールにすることで，今後のチップ・セットの改良や各国の法規制などへの対応を容易にする．

(multiband-orthogonal frequency division modulation)シンボルを含んでいます(**図5**).

Wireless USBでは，MMCとCTAのタイミングを測定することは重要です．プロトコル・アナライザを用いて，実際のMMCやCTAのタイミングの間隔が期待値を超えていないかどうかを確認します(**図6**).

2．アソシエーション・モデル

すでに述べたように，Wireless USBでは最初にホストとデバイスを接続する際の処理手順として「アソシエーション・モデル」が規定されています．一度アソシエーション・モデルにのっとってお互いを確認した後は，ほかの機器と干渉することなく，安全に通信を行えます.

● USB-IFの定める方式は「ケーブル式」と「数値方式」

そのためアソシエーションには，しっかりとしたセキュリティと使いやすさが求められています．また，追加コストをできるだけ抑えることも重要なポイントです．これらの要求を踏まえ，2006年3月にUSB-IFにて「Association Models Supplement to the Certified Wireless Universal Serial Bus Specification Revision 1.0」が承認され，有線認証方式(cable model)と数値入力方式(numeric model)の二つのアソシエーション・モデルが決められました(2).

ホストは，有線認証方式と数値入力方式の両方のアソシエーション・モデルに対応する必要があります．USBポートを備えているデバイスは有線認証方式のモデルに，表示機能を備えたデバイスは数値入力方式のモデルに対応しなければなりません(デバイスは二つの方式のうちどちらかに対応していればよい).

有線認証方式の手順は次のとおりです．まず，デバイスとホストをUSBケーブルで接続します．すると，ホストは「接続成功！ このデバイスをワイヤレスで使えます(Success！ You may now use this device wirelessly)」というメッセージを出します．USBケーブルを外せば，これでアソシエーションは完了です．それ以降は，ケーブル接続する必要はありません.

次に数値入力方式の手順ですが，まずデバイスをホスト

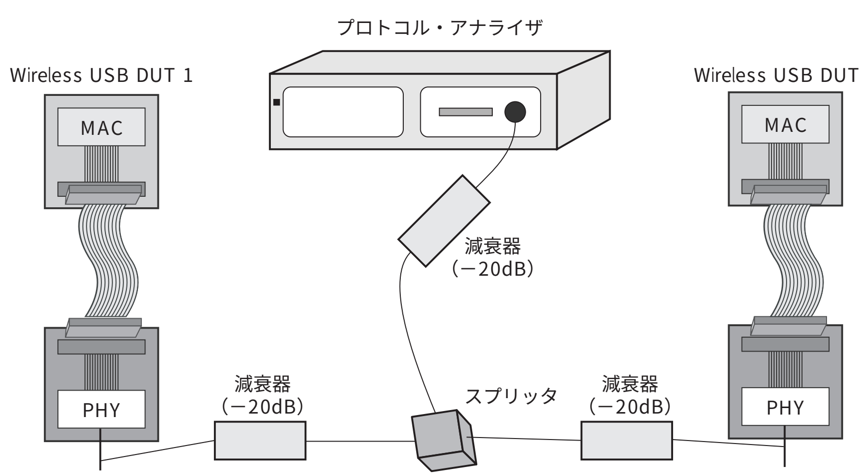


図3
同軸ケーブルによるデータ捕捉
ノイズの多いテスト環境では，SMAケーブルで直接接続してデータを捕捉する.

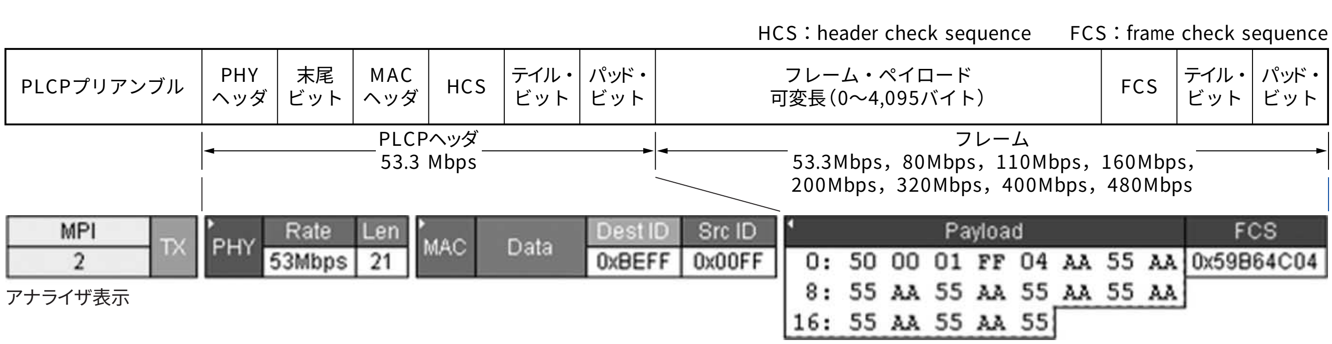
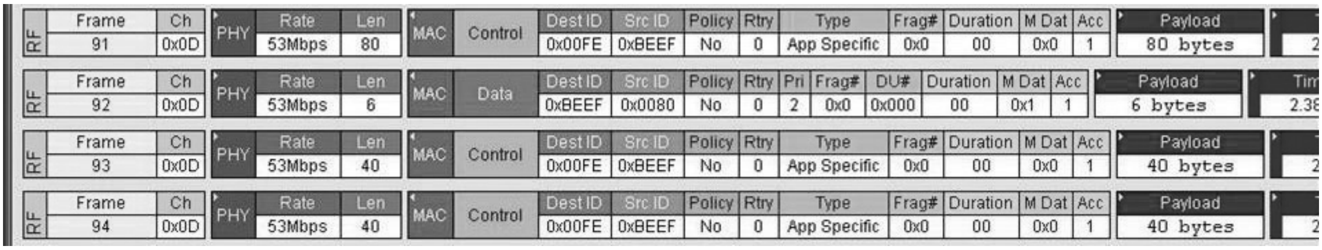
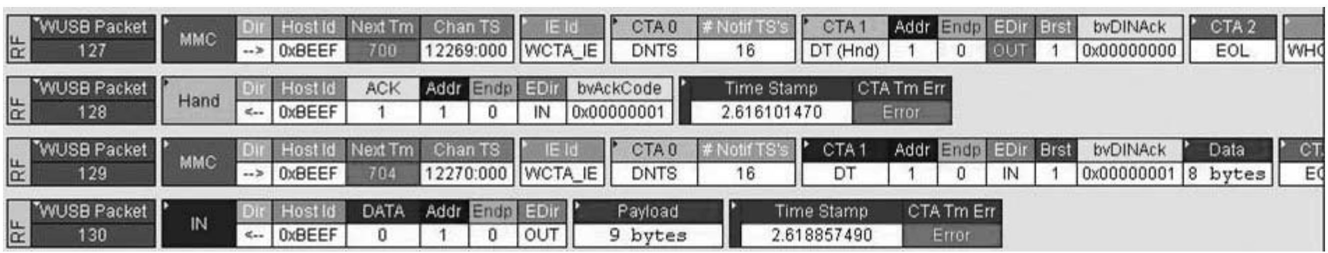


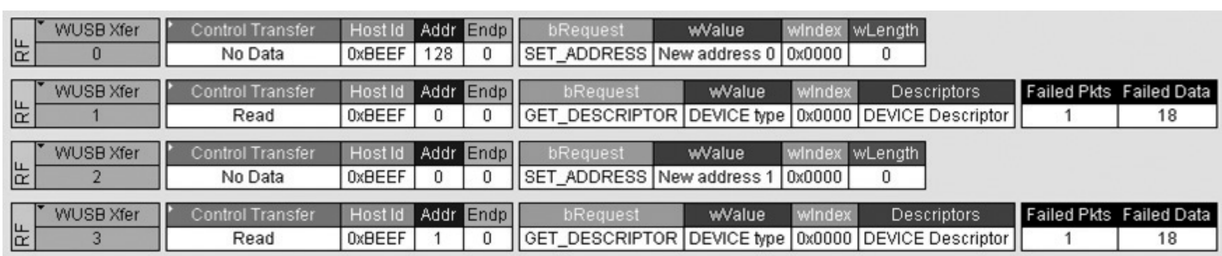
図4 Wireless USBのパケットとアナライザ表示



(**a**) MPI



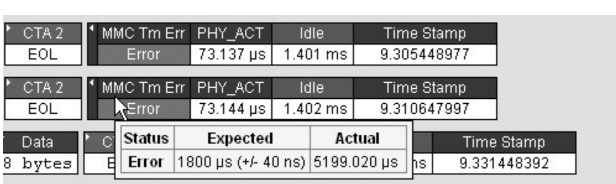
(**b**) パケット層



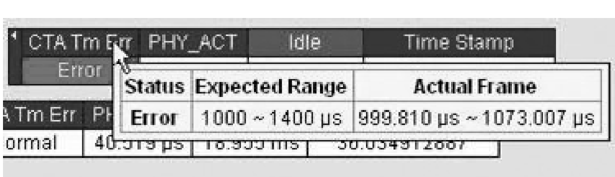
(**c**) トランスファ層

図5　各階層におけるアナライザ表示

(a)に物理層，MAC層の，(b)にパケット層の，(c)にトランスファ層のデータの表示例を示す．



(**a**) MMC



(**b**) CTA

図6　タイミング検証

LeCroy社の「UWB Tracer」を用いて，タイミング検証を行った例．タイミングが期待値を超えた場合，ソフトウェアのエラー・フラグが設定される．エラー・レポート機能を備えており，プロトコルのすべての階層において自動的にエラーを検出する．

の近くに持ってきます．ホスト(パソコン)のメニュー表示から「新しいデバイスの追加(add a new device)」という項目を選択します．デバイスはメニュー表示から「新しいホストに接続(connect to new host)」という項目を選択します．すると，ホストの表示部にコード(数値)が現れ，デバイスの表示部にも同じコードが現れます．そのコードを比較し同一であることを確認できたら，ホストとデバイスそれぞれの表示部にて「認証(accept)」を選択します．すると，有線認証方式の場合と同じく，ホストの表示部に「接続成功！ このデバイスをワイヤレスで使えます(Success！ You may now use this device wirelessly)」というメッセージが出されます．これでアソシエーションは完了です．

● セキュアなデータに対するプロトコル解析

Wireless USBはアソシエーション・モデルのほかに,

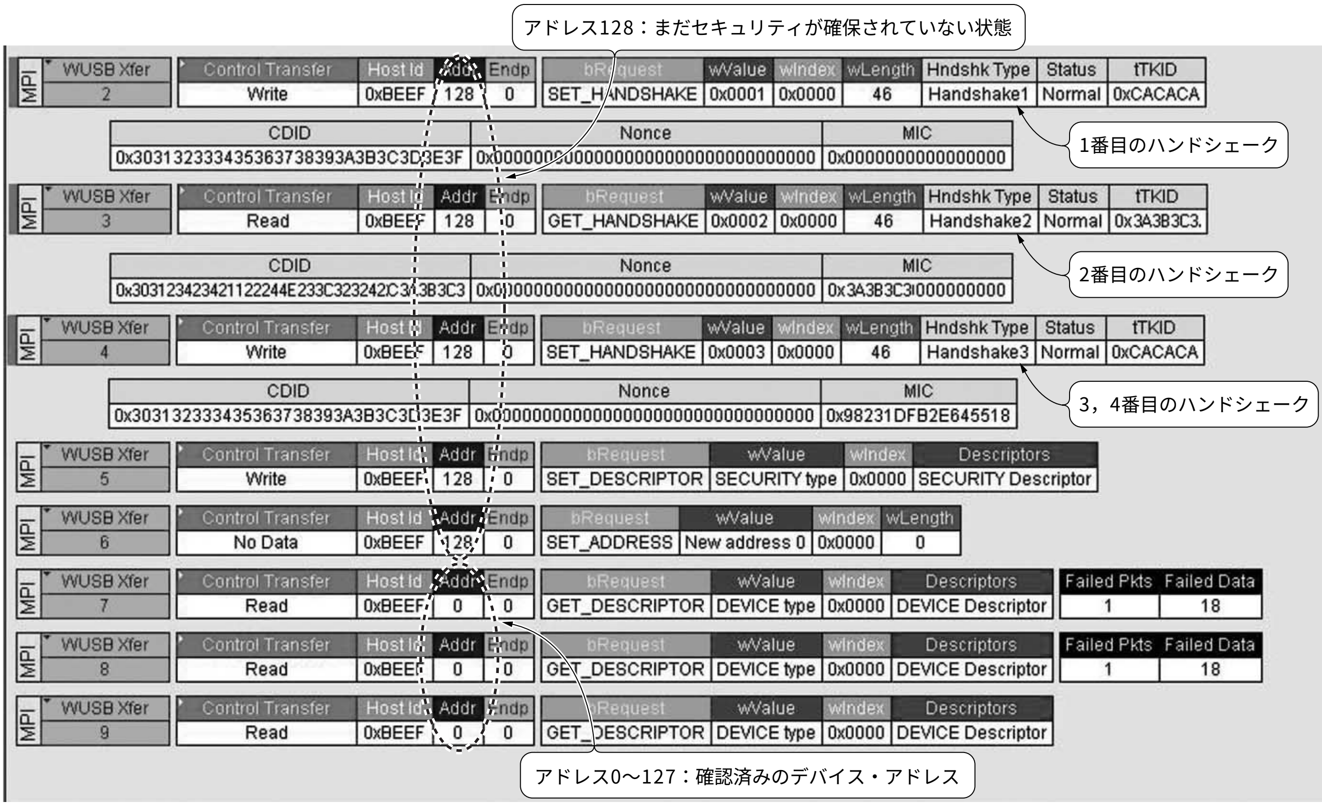


図8　4-Way暗号化ハンドシェークの表示例
セキュリティが確立できた場合，アドレスは0～127の範囲になる．

セキュリティ・モデルが規定されています．上述したように，アソシエーションはホストとデバイスの間で接続コンテキスト（数値列）を交換するもので最初に一度行えばよいのですが，セキュリティは暗号化されたパケットのやりとりを継続的に行います．

有線認証方式のアソシエーション・モデルの場合，最初にデバイスはUSBケーブルを経由して接続コンテキスト交換します．接続コンテキストを捕捉した後，アナライザは一時キー（PTK：pairwise temporal key）を引き出すことができます．

数値入力方式のアソシエーション・モデルでは，デバイスがアソシエーションを開始すると，デバイスがハッシュ関数の計算を行い，公開鍵の交換を行います．共有の暗号鍵を計算し，ユーザが数値を入力して認証が行われます．数値の一致が確認されて，接続コンテキストが確立します．

数値入力方式は，数値認証の際にユーザが介入する必要があり，盗み見される可能性があります．そのため有線認証方式と比べてセキュアではありませんが，無線通信データの暗号化によってセキュリティを維持します．無線通信データが暗号化されると，パケットそのものは捕捉できるのですが，具体的なデータの内容を解析できなくなります．プロトコル検証を行うには，暗号を外したデータの取得が必要です．

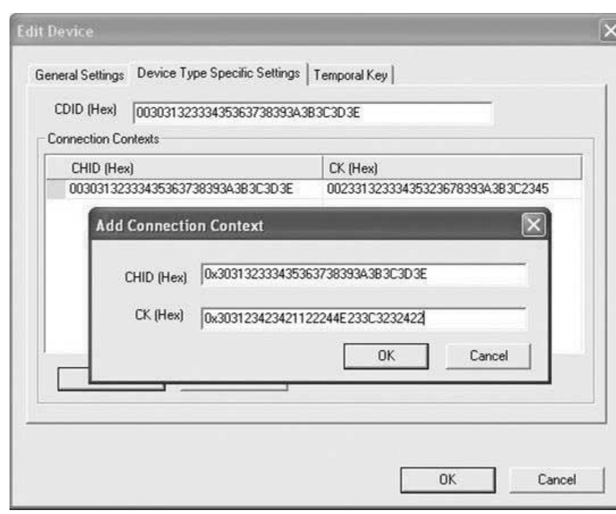


図7　接続コンテキストの暗号鍵をマニュアルで追加
アソシエーションを確立するため，接続コンテキスト・キーを入力する．

そこで，例えば接続コンテキストの暗号鍵を追加するこ

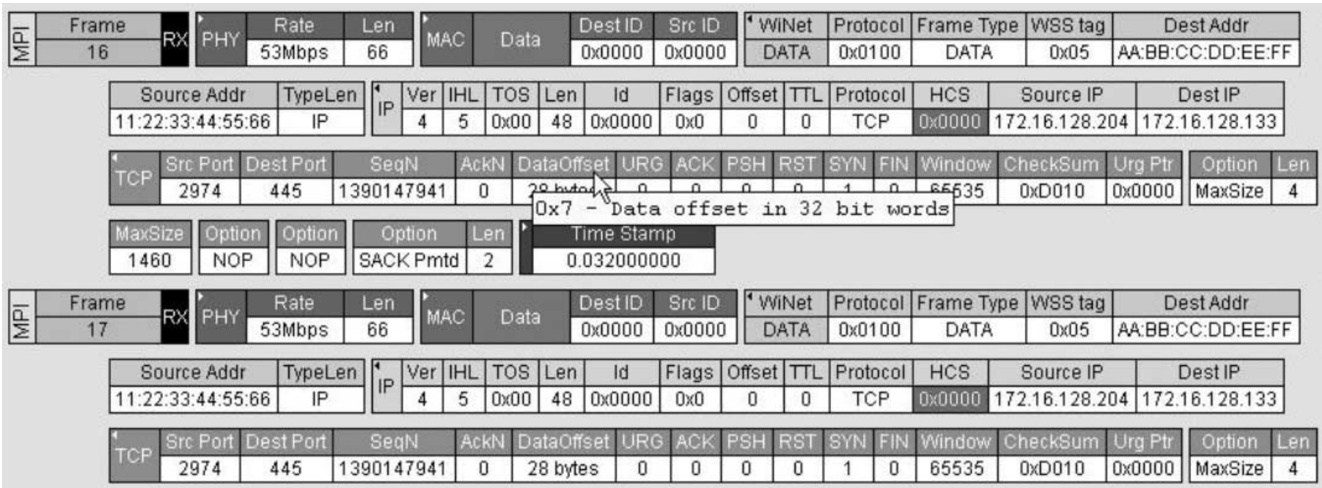


図9　WiNETプロトコルの解析
LeCroy社の「UWB Tracer」のWiNETオプションにて，TCPとIPのヘッダ・フィールドのデコードも可能．

とでTK（temporal key）を取り出し，暗号化されたパケットのデコードを行う機能を備えたプロトコル・アナライザを利用します（**図7**）．

上述したような接続コンテキストを用いた認証手段を，Wireless USB仕様では「4-Wayハンドシェーク」と呼びます．4-Wayハンドシェークは，アソシエーションが完了した後でも必要です（**図8**）．情報アクセスの資格検証，つまり正しいユーザであることの確認が一度確立できたら，デバイスはNAKなどをセキュリティ確認のための時間期限（trust timeout window）である4秒以内に交換しなければなりません．もし接続が切れると，デバイスは再接続要求をホストに送らなければなりません．ホストの再認証とTKの再発行を行う仕組みにより，セキュアな通信が保たれるのです．プロトコル・アナライザには，このタイムアウトの信頼性の検証を容易にする高度なトリガ機能も必要となります．

● UWBをベースとしたほかのプロトコルへの広がり

WiMedia Allianceが策定するUWB無線プラットホーム（common radio platform）では，USBのほかにIP（internet protocol）にも対応する仕組みになっています．これはWiNETと呼ばれる規格で，PAL（protocol adaptation layer）を介してIPパケットを無線化するものです．次世代のパソコンのOSではWireless USBとともにWiNETも搭載されることが検討されています．WiNETの検証にもプロトコル・アナライザは強力なツールになると予想されます（**図9**）．

参考・引用*文献

(1) USB-IF；Wireless Universal Serial Bus Specification, May 12, 2005.（http://www.usb.org/wusb/から入手可能）
(2) USB-IF；Association Models Supplement to the Certified Wireless Universal Serial Bus Specification, Mar. 2, 2006.（http://www.usb.org/wusb/から入手可能）
(3) LeCroy；LeCroy UWB Tracer（Ultra-Wideband Protocol Analyzer）User Manual.（http://www.lecroy.com/tm/library/manuals/から入手可能）
(4) レクロイ・ジャパン；WiMediaとCertified Wireless USBのプロトコル検証の紹介，レクロイ・ジャパン主催第4回ワイヤレスUSB講演会資料，2006年7月21日.（http://www.lecroy.com/japan/pdf/semi/から入手可能）
(5) 辻 嘉樹；Certified Wireless USB対応機器の検証の勘どころ，Design Wave Magazine，2006年11月号，pp.98-113.

ふくざき・たつや
レクロイ・ジャパン（株）

<筆者プロフィール>
福崎達也．2002年にレクロイ・ジャパンに入社．マーケティング・マネージャとして従事．前職は大手家電メーカの半導体事業部にて，高速インターフェースICの設計開発と，その標準化に努めた．